

## Article - State Government

[\[Previous\]](#)[\[Next\]](#)

§10–13A–03.NOT IN EFFECT

**\*\* TAKES EFFECT OCTOBER 1, 2024 PER CHAPTER 429 OF 2020 \*\***

(a) Each public institution of higher education shall review and designate systems within the public institution of higher education as systems of record based on the following criteria:

(1) the risk posed to individuals by the personally identifiable information processed and stored on the systems;

(2) the relationship of the systems to the overall function of the public institution of higher education; and

(3) the technical and financial feasibility of implementing privacy controls and services within the system.

(b) Each public institution of higher education shall develop and adopt a privacy governance program to govern each system of record that:

(1) identifies and documents the purpose of the public institution of higher education in processing personally identifiable information;

(2) prohibits the disclosure of personally identifiable information to third parties, other than those third parties processing personally identifiable information on behalf of the public institution of higher education, unless:

(i) the individual consents to disclosure of the information; or

(ii) the public institution of higher education determines that disclosure of the information is in the best interest of the public institution of higher education;

(3) requires all agreements entered into with third parties on or after October 1, 2024, to include language requiring the third party to support the privacy governance program of the public institution of higher education;

(4) ensures that a third party processing personally identifiable information on behalf of the public institution of higher education acts in accordance with the privacy governance program of the public institution of higher education;

(5) takes reasonable steps to ensure that personally identifiable information processed by the public institution of higher education is accurate, relevant, timely, and complete;

(6) takes reasonable steps to ensure that requests to access, modify, or delete information and requests to opt out of the sharing of information with third parties are made by the subject of the personally identifiable information or the subject's agent;

(7) takes reasonable steps to limit the personally identifiable information collected to that information necessary to address the purpose of the collection;

(8) implements a process to provide individuals with access to the personally identifiable information relating to the individual held and processed by the public institution of higher education;

(9) provides individuals with a process to request a correction to personally identifiable information relating to the individual;

(10) in the case of a disagreement between the public institution of higher education and an individual over the accuracy of personally identifiable information relating to the individual, provides a means for the individual to document the disagreement and produce the documentation of the disagreement whenever the disputed information is produced;

(11) provides a process for individuals to request the deletion of personally identifiable information relating to the individual that the public institution of higher education does not have a legitimate basis to process;

(12) provides a process for individuals to opt out of sharing personally identifiable information relating to the individual with third parties, if the public institution of higher education would not have a legitimate basis to process the information; and

(13) provides a process for the public institution of higher education to consider requests made under this subsection that allows the public institution of higher education to deny a request if the public institution of higher education reasonably concludes it has a legitimate basis for processing the personally identifiable information or if the request is not technically or financially feasible.

(c) Each public institution of higher education shall develop and adopt an information security and risk management program for the protection of personally identifiable information that shall:

(1) implement reasonable security procedures and practices, compatible with applicable federal and State standards and guidelines, to ensure that the risk to the confidentiality, integrity, and availability of all personally identifiable information is properly managed;

(2) be periodically assessed by a third party assessor with expertise in information security;

(3) be approved by an appropriate senior official of the public institution of higher education with authority to accept risk for the public institution of higher education;

(4) require that contracts with third parties include provisions to ensure that third parties that process personally identifiable information on behalf of the public institution of higher education maintain appropriate security controls commensurate with the risk posed to the individuals by the personally identifiable information; and

(5) ensure that any breaches by the public institution of higher education or a third party acting on behalf of the public institution of higher education are properly documented, investigated, and reported to appropriate authorities within the public institution of higher education.

(d) (1) Each public institution of higher education shall publish a privacy notice on the website of the public institution of higher education that is:

(i) written in plain language; and

(ii) directly accessible from the homepage and any of the webpages of the public institution of higher education that are used to collect personally identifiable information.

(2) The notice published under paragraph (1) of this subsection shall include:

(i) the types of personally identifiable information collected by the public institution of higher education;

(ii) the purpose of the collection, use, and sharing of personally identifiable information by the public institution of higher education; and

(iii) the processes by which an individual may request:

1. to have personally identifiable information related to the individual corrected;
2. to have personally identifiable information related to the individual deleted;
3. information on the sharing of personally identifiable information by the public institution of higher education with third parties, including a listing of the third parties, a listing of the information shared, and the purpose of sharing the information; and
4. to opt out of the sharing of personally identifiable information with a third party.

(3) Each public institution of higher education shall ensure access controls are in place to address any security risks posed by providing the notice required under this subsection.

(e) When a public institution of higher education is destroying records of an individual that contain personally identifiable information of the individual, the public institution of higher education shall take reasonable steps to protect against unauthorized access to or use of the personally identifiable information, taking into account:

- (1) the sensitivity of the records;
- (2) the nature of the public institution of higher education and its operations;
- (3) the costs and benefits of different destruction methods; and
- (4) available technology.

(f) Each public institution of higher education shall develop and adopt a policy establishing an appropriate remedy for individuals whose personally identifiable information has been affected by a breach.

[\[Previous\]](#)[\[Next\]](#)